

VERSION 3.5

Novell BorderManager

Authentication Services



BorderManagerTM
ENTERPRISE EDITION 3

Novell[®]

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

The Harvest software was developed by the Internet Research Task Force Research Group on Resource Discovery (IRTF-RD):

Mic Bowman of Transarc Corporation.
Peter Danzig of the University of Southern California.
Darren R. Hardy of the University of Colorado at Boulder.
Udi Manber of the University of Arizona.
Michael F. Schwartz of the University of Colorado at Boulder.
Duane Wessels of the University of Colorado at Boulder.

Copyright © 1994, 1995, Internet Research Task Force Research Group on Resource Discovery. All rights reserved. This copyright notice applies to software in the Harvest “src/” directory only. Users should consult the individual copyright notices in the “components/” subdirectories for copyright information about other software bundled with the Harvest source code distribution.

Copyright © 1999 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent Nos. 5,553,139; 5,553,143; 5,572,528; 5,719,786; 5,758,069; 5,818,936; 5,903,650; 5,905,860. U.S. and Foreign Patents Pending.

**Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.**

www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

**Novell BorderManager Authentication Services
June 1999**

TERMS OF USE

The Harvest software may be used and redistributed without charge, provided that the software origin and research team are cited in any use of the system. Most commonly, this is accomplished by including a link to the Harvest Home Page (<http://harvest.cs.colorado.edu/>) from the query page of any Broker you deploy, as well as in the query result pages. These links are generated automatically by the standard Broker software distribution.

The Harvest software is provided “as is,” without express or implied warranty, and with no support nor obligation to assist in its use, correction, modification or enhancement. We assume no liability with respect to the infringement of copyrights, trade secrets, or any patents, and are not responsible for consequential damages. Proper use of the Harvest software is entirely the responsibility of the user.

DERIVATIVE WORKS

Users may make derivative works from the Harvest software, subject to the following constraints:

— You must include the above copyright notice and these accompanying paragraphs in all forms of derivative works, and any documentation and other materials related to such distribution and use must acknowledge that the software was developed at the above institutions.

— You must notify IRTF-RD regarding your distribution of the derivative work.

— You must clearly notify users that you are distributing a modified version and not the original Harvest software.

— Any derivative product is also subject to these copyright and use restrictions.

Note that the Harvest software is NOT in the public domain. We retain copyright, as specified above.

HISTORY OF FREE SOFTWARE STATUS

Originally we required sites to license the software in cases in which they were going to build commercial products/services around Harvest. In June 1995, we changed this policy. We now allow people to use the core Harvest software (the code found in the Harvest “src/” directory) for free. We made this change in the interest of encouraging the widest possible deployment of the technology. The Harvest software is really a reference implementation of a set of protocols and formats, some of which we intend to standardize. We encourage commercial reimplementations of code complying to this set of standards.

*export
notice*

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

LANalyzer, LAN WorkPlace, Novell, and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. BorderManager, Client 32, ConsoleOne, Internetwork Packet Exchange, IPX, NASI, NCP, NDPS, NDS, NetWare 5, NetWare Asynchronous Services Interface, NetWare Connect, NetWare Core Protocol, NetWare/IP, NetWare Link Services Protocol, NetWare Loadable Module, NetWare MultiProtocol Router, NLM, NLSP, Novell BorderManager, Novell BorderManager FastCache, Novell Client, Novell Distributed Print Services, Virtual Loadable Module, VLM, and Z.E.N.works are trademarks of Novell, Inc.

AppleTalk is a registered trademark of Apple Computer, Inc.
Btrieve is a registered trademark of Pervasive Software, Inc.
Cyber Patrol is a registered trademark of Learning Company Properties, Inc.
CyberNOT is a trademark of Learning Company Properties, Inc.
CyberNOT List is a trademark of Learning Company Properties, Inc.
CyberNOT is a trademark of Learning Company Properties, Inc.
CyberYES List is a trademark of Learning Company Properties, Inc.
Hayes is a registered trademark of Hayes Microcomputer Products, Inc.
Java is a trademark of Sun Microsystems, Inc. in the United States and other countries.
JavaScript is a trademark of Sun Microsystems, Inc.
Macintosh is a registered trademark of Apple Computer, Inc.
Microsoft is a registered trademark of Microsoft Corporation.
NCSA is a registered trademark of Bales, Gates & Associates, Inc.
Netscape is a registered trademark of Netscape Communications Corporation.
Netscape Communicator is a registered trademark of Netscape Communications Corporation.
Netscape Navigator is a registered trademark of Netscape Communications Corporation.
OS/2 is a registered trademark of International Business Machines Corporation.
PS/2 is a registered trademark of International Business Machines Corporation.
Pentium is a registered trademark of Intel Corporation.
RealAudio is a registered trademark of RealNetworks, Inc.
RealPlayer is a registered trademark of RealNetworks, Inc.
RealVideo is a registered trademark of RealNetworks, Inc.
The Learning Company is a registered trademark of Learning Company Properties, Inc.
UNIX is a registered trademark of X/Open Company, Ltd.

USRobotics is a registered trademark of U.S. Robotics, Inc.
WebTrends is a trademark of WebTrends Corporation.
Windows is a registered trademark of Microsoft Corporation.
Windows 95 is a trademark of Microsoft Corporation.
Windows 98 is a trademark of Microsoft Corporation.
Windows NT is a registered trademark of Microsoft Corporation.
X Window System is a trademark of Massachusetts Institute of Technology.

The RSA logo is a trademark of RSA Data Security, Inc.



Contents

About This Guide

1 Advanced Configuration of Authentication Services

Changing RADIUS Server Options	1
Setting Up Dial Access Services	3
Creating and Setting Up Dial Access System Objects	3
Creating Dial Access Profile Objects	5
Creating and Setting Up User Objects	6
Setting Up Users and Groups for Container and Group Administration.	8
Setting Up Organization and Organizational Unit Container Objects	8
Setting Up Group Objects	10
Setting Up Remote Connection Restrictions	12
Specifying Dial Access System Login Restrictions	12
Specifying Per-User Login Restrictions	14
Planning Token Authentication	15
Authentication Container Object.	16
Authentication Device Object	16
Protecting Device Data in NDS	17
Managing Token Authentication	18
Creating an Authentication Container Object	18
Creating an Authentication Device Object.	19
Importing a Token	19
Manually Initializing a Token	19
Locally Initializing a Token	20
Assigning a Single Token	20
Assigning a Series of Tokens	21
Synchronizing a Token	21
Unlocking a Token.	21
Testing Passwords	22
Planning Authentication Policies	22
Authentication Device Manager	23
Authentication Policy Object.	23
Supported Authentication Methods	24
Authentication Rules	25

Setting Up Authentication Policies	26
Creating an Authentication Policy Object	27
Defining the Server to Host the Authentication Policy Object	27
Configuring Authentication Policy Rules	27
Planning RADIUS Proxy Services	28
Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS Context to Any RADIUS Server	31
Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS Context to a Specific RADIUS Server	32
Setting Up a RADIUS Authentication Proxy as an ISP to Forward Requests to a Corporate RADIUS Server	32
Setting Up a RADIUS Authentication Proxy to Forward Requests to a Third-Party Authentication Server Supporting Token Authentication .	33
Setting Up a RADIUS Authentication Proxy to Forward Requests to Third-Party Authentication Server Supporting Token Authentication with Token Serial Numbers as Usernames	34
Setting Up a RADIUS Authentication Proxy to Authenticate Usernames to a Search Domain	34
Managing RADIUS Proxy Services	35
Adding an NDS Context Domain Processed by Any RADIUS Server	36
Adding an NDS Context Domain Processed by a Specific RADIUS Server .	36
Adding a Generic Proxy Server Domain	37
Adding a Search Domain Server Domain	37
Adding a RADIUS Accounting Proxy Domain	38
Adding an External Authentication Service Object	38
Adding an External Identity Object	39
Modifying a Domain	39
Deleting a Domain	39
Displaying RADIUS Status Messages	40
Access Rejected Messages	40
Message Dropped Messages	44
Other Messages	44

About This Guide

Novell® BorderManager™ Enterprise Edition Installation and Setup provides the basic information you need to set up BorderManager Authentication Services.

This documentation provides the following additional information: “Advanced Configuration of Authentication Services” on page 1—This chapter describes configuration procedures for setting up additional features available with BorderManager Authentication Services.

1 ***Advanced Configuration of Authentication Services***

This chapter describes advanced configuration procedures for Novell® BorderManager™ Authentication Services. It contains the following sections:

- “Changing RADIUS Server Options” on page 1
- “Setting Up Dial Access Services” on page 3
- “Setting Up Users and Groups for Container and Group Administration” on page 8
- “Setting Up Remote Connection Restrictions” on page 12
- “Planning Token Authentication” on page 15
- “Managing Token Authentication” on page 18
- “Planning Authentication Policies” on page 22
- “Setting Up Authentication Policies” on page 26
- “Planning RADIUS Proxy Services” on page 28
- “Managing RADIUS Proxy Services” on page 35
- “Displaying RADIUS Status Messages” on page 40

Changing RADIUS Server Options

You can change Remote Dial-In User Services (RADIUS) server options from the NetWare® server command line, including the distinguished name of the Dial Access System object and the Dial Access System password for the specified Dial Access System object.

LOAD RADIUS

[name = Dial Access System distinguished name] [password = Dial Access System password] [threads = number of threads] [port = UDP port number for RADIUS] [acctPath = RADIUS accounting directory] [fileFormat = [standard|comma]] [rollOver = [daily|weekly|monthly]] [serverType = [accounting|authentication] [decrementGraceLogins = [YES|NO]

All parameters are optional. The values you specify override the default values.

If you do not specify the name or password on the command line, you will be prompted to provide a name and password at startup. Names can be specified as relative distinguished names, distinguished names, or partial distinguished names. Both typed and typeless names are supported. Refer to the NDS™ documentation for details on specifying names.

The default context is set to the current bindery context. After Novell® BorderManager™ Authentication Services has been loaded, the default context is set to the Dial Access System name context.

Strings with embedded spaces must be contained in quotation marks. In addition, a quoted parameter must be preceded with a space.

The valid values for the number of threads range between 1 and 127. The default number of threads is 5, which should be satisfactory in most cases.

The default UDP port number is 1645 (the most commonly used). However, a new UDP port number (1812) has been assigned by the Internet Engineering Task Force (IETF) for RADIUS services.

The default path for the RADIUS accounting files is
SYS:\ETC\RADIUS\ACCT.

The RADIUS accounting server is typically implemented as a separate process of the RADIUS authentication server. The RADIUS accounting server listens on UDP port number 1813. When an accounting packet is received from a RADIUS client (such as a network access server), the RADIUS accounting server logs the information in an ASCII text file and returns an acknowledgment to the RADIUS client.

The default RADIUS accounting file format is comma-delimited text (standard ASCII file format is optional).

The default period before a RADIUS accounting file is rolled over is daily (weekly and monthly are optional).

By default, the BorderManager Authentication Services software runs both the authentication server and the accounting server when you do not specify the `ServerType` option on the command line. (Running just the authentication server or the accounting server is optional.)

By default, the BorderManager Authentication Services software does not decrement grace logins.

Setting Up Dial Access Services

You must perform the following tasks to create and set up the necessary NDS™ objects in your NDS tree to support dial access services with Novell® BorderManager™ Authentication Services:

- “Creating and Setting Up Dial Access System Objects” on page 3
- “Creating Dial Access Profile Objects” on page 5
- “Creating and Setting Up User Objects” on page 6

Creating and Setting Up Dial Access System Objects

You must create a Dial Access System object in your NDS tree to manage common configuration tasks for a collection of RADIUS servers working together. The information stored in this object consists of the following:

- Client configuration—Enables you to define IP addresses for network access servers and shared secrets among the RADIUS servers and the various network access servers.
- Domains—Enables you to configure other RADIUS servers to which you want to forward RADIUS requests.
- Authentication policy—Enables you to define the authentication policy for the Dial Access System object.
- Dial Access System object password—Enables you to restrict access to authorized users.
- Lookup contexts—Enables contexts to be searched when the common name portion of the username is received in an authentication request.

- Remote connection restrictions—Enables you to limit the number of connections that a remote user can have concurrently per network.

Typically, you need only one Dial Access System object in your NDS tree.

You can easily assign rights to an NDS object using NetWare® Administrator. For example, you can assign Browse and Read rights from NetWare Administrator by dragging the Dial Access System object over an Organizational Unit object near the root of an NDS tree.

This section contains the following tasks:

- “Creating a Dial Access System Object” on page 4
- “Configuring a Dial Access System Object” on page 4
- “Specifying a Dial Access System Password” on page 5

Creating a Dial Access System Object

To create a Dial Access System object, complete the following steps:

1. **In NetWare® Administrator, select the Organizational Unit container object.**
2. **Select Object > Create > Dial Access System.**
3. **Enter the name of the Dial Access System object and click Create.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Configuring a Dial Access System Object

To configure a Dial Access System object, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Clients > Add to add a RADIUS client. Enter the following information:**
 - IP address of the network access server
 - Client type

- RADIUS secret
3. **Select Authentication Policy > Add to configure an authentication policy. Specify the following information:**
 - Policy type
 - Policy rules
 4. **Select Lookup Context > Add if you want to use common name login. Browse and select the name context, then click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Specifying a Dial Access System Password

To specify a Dial Access System password, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Miscellaneous > Change Dial Access System Password.**
3. **Enter and reenter the new password, then click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Creating Dial Access Profile Objects

You must create at least one Dial Access Profile object in your NDS tree to define common services used by many dial-in users. The Dial Access Profile object contains a list of RADIUS dial access attributes that specify the configuration for creating a specific service.

You can set up as many profiles as you need to define different services. For example, you can create a Point-to-Point Protocol (PPP) profile that enables users to dial in and access the Internet. You can also create a Telnet profile that enables users to connect to a local host using a terminal or terminal emulator. You can specify dial access profiles in the User object that can override settings in the Dial Access Profile object.

Creating a Dial Access Profile Object

To create a Dial Access Profile object, complete the following steps:

1. **In NetWare Administrator, select the Organizational Unit container object.**
2. **Select Object > Create > Dial Access Profile.**
3. **Enter the name of the Dial Access Profile object and click Create.**
4. **Select the Dial Access Profile object you created > Attributes > Add and specify RADIUS attributes.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Creating and Setting Up User Objects

The User Dial Access Services page allows you to

- Enable a user for dial access services
- Select the appropriate Dial Access System object for a user
- Set a Dial Access System Password for a user (if you use separate passwords for dial-in users)
- Configure (or define) dial-in services for a user (such as enabling a user to select one or more Dial Access Profile objects and associate user-specific settings for each)
- Select a default dial access service if a user is configured for more than one
- Configure remote connection restrictions as well as view active connections and connection history
- Assign an authentication device

This section contains the following tasks:

- “Enabling a User Object for Dial Access Services” on page 7

- “Disabling Dial Access Services for a User Object” on page 7
- “Adding a User's Token Assignment” on page 7
- “Deleting a User's Token Assignment” on page 8

Enabling a User Object for Dial Access Services

To enable a User object for dial access services, complete the following steps:

- 1. In NetWare Administrator, select the User object.**
- 2. Select Dial Access Services, specify a dial access control setting, and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Disabling Dial Access Services for a User Object

To disable a User object for dial access services, complete the following steps:

- 1. In NetWare Administrator, select the User object.**
- 2. Select Dial Access Services > Select Disable, then click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding a User's Token Assignment

To add an Authentication Device assignment, complete the following steps:

- 1. In NetWare Administrator, select the User object.**
- 2. Select Authentication Devices > Add.**
- 3. Browse to the context containing the object to assign, select the object, and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Deleting a User's Token Assignment

To delete an Authentication Device assignment, complete the following steps:

1. **In NetWare Administrator, select the User object.**
2. **Select Authentication Devices.**
3. **Select the device to delete, then click Delete > OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting Up Users and Groups for Container and Group Administration

Perform the following tasks to modify the NDS™ objects in your NDS tree to manage dial access services with Novell® BorderManager™ Authentication Services:

- “Setting Up Organization and Organizational Unit Container Objects” on page 8
- “Setting Up Group Objects” on page 10

Setting Up Organization and Organizational Unit Container Objects

You can specify common dial access properties for all users in Organization or Organizational Unit container objects. The Dial Access Service page of an Organization or Organizational Unit allows you to

- Enable dial access services for all users
- Select the Dial Access System object for all users
- Configure the dial access services that can be used by all users in a container

For example, if your organization has several departments that want to allow remote users to access your corporate network, you could use BorderManager Authentication Services to manage users who authenticate with the RADIUS

protocol. Each department could specify rights to applications, file and print services, and dial-in configuration information. However, multiple departments could be managed by the same network administrator without the requirement to maintain multiple databases.

Specifying dial access properties in the Dial Access Service page for an Organization or Organizational Unit container object has the following benefits:

- Configuring all users in an Organization or Organizational Unit to have the same dial-in rights simplifies administration over per-user administration.
- Configuring users in different containers with different access rights enhances security.

The dial access properties that you define for an Organization or Organizational Unit container object apply to every user in the selected container object (but not to users in Organizational Units that are at a lower level in the NDS tree). Refer to the NetWare® Administrator online help for information about specific configuration procedures.

You can override the dial access properties of an Organization container object or Organizational Unit container object by modifying the Dial Access Services page of a User object. This allows you to specify unique dial access properties for any User object in your NDS tree.

Enabling Dial Access Services For Users in a Container Object

To enable users in an Organization or Organizational Unit container object for dial access services, complete the following steps:

- 1. In NetWare Administrator, select the Organization or Organizational Unit container object.**
- 2. Select Dial Access Services > Enable Dial Access and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting Up Group Objects

You can grant rights to use one or more specified Dial Access System objects to members of a Group object. Group-based administration leverages the powerful access control list (ACL) capability of NDS to enforce user dial-in access restrictions. For example, separate Dial Access System objects could be created for firewall and dial-in access servers. Then a Firewall Group object and a Dial-In Users Group object could be created with access privileges to the firewall Dial Access System object and the dial-in Dial Access System object. By making a user a member of one or both groups, access to these resources is granted selectively based on group membership. Group-based administration can also be used to allow access to high-speed connections by selected users only, while allowing low-speed connections by all users by creating multiple Dial Access System objects.

Restricting access based on assignment to a geographical region is another use for group-based administration. Dial Access System objects could be created for each geographical region that a set of users are allowed to access. Groups such as West Coast, Midwest, and East Coast could be created with users in those regions added as members. Certain users, such as sales staff, could be included in more than one geographical group to allow access to different locations.

Each Dial Access System object must have sufficient rights to any User object that can be authenticated. This can be done for multiple users in a Group object by assigning a parent container object to which the users belong as a trustee of a Dial Access System object.

Likewise, the Group object must have sufficient rights to the Dial Access System object used for authentication. This can be done by assigning the Group object as a trustee of the Dial Access System object.

This section contains the following tasks:

- “Assigning a Container Object as a Trustee of a Dial Access System Object” on page 11
- “Assigning a Group Object as a Trustee of a Dial Access System Object” on page 11

Assigning a Container Object as a Trustee of a Dial Access System Object

To assign a container object as a trustee of a Dial Access System object, complete the following steps:

- 1. In NetWare Administrator, select the Dial Access System object.**
- 2. Select Object > Trustees Of This Object > Add Trustees.**
- 3. Select the Organization or Organizational Unit container object and check the following properties:**
 - Object Rights>Browse
 - Property Rights>All Properties>Read
 - Property Rights>All Properties>Write
- 4. Click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Assigning a Group Object as a Trustee of a Dial Access System Object

To assign a group object as a trustee of a Dial Access System object, complete the following steps:

- 1. In NetWare Administrator, select the Dial Access System object.**
- 2. Select Object > Trustees Of This Object > Add Trustees.**
- 3. Select the Group object and check the following properties:**
 - Object Rights>Browse
 - Property Rights>All Properties>Read
 - Property Rights>All Properties>Write
- 4. Click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting Up Remote Connection Restrictions

You can limit the number of connections that a remote user can have concurrently per network. You can restrict the number of concurrent dial-in connections for each User object, or you can set a default value for concurrent dial-in connections for each Dial Access System object.

This section contains the following tasks:

- “Specifying Dial Access System Login Restrictions” on page 12
- “Specifying Per-User Login Restrictions” on page 14

Specifying Dial Access System Login Restrictions

By default, the RADIUS server allows unlimited dial-in connections. You can also specify the number of concurrent dial-in connections that the RADIUS server will allow for each User object that authenticates through a given Dial Access System object.

For a given Dial Access System object, you can specify the following types of information tracked for each dial-in user:

- Timeout interval for an interim accounting packet (determines if a dial-in connection is active)
- Time interval (in days) before an entry in a user's current login connection is removed
- Maximum number of records kept in a user's login connection history

This section contains the following tasks:

- “Setting Dial Access System Remote Connection Restrictions” on page 13
- “Setting the Current Connection Interval” on page 13
- “Setting the Interim Accounting Timeout Interval” on page 13
- “Setting the Maximum Records in the Remote Connection History” on page 14

Setting Dial Access System Remote Connection Restrictions

To add remote connection restrictions, complete the following steps:

1. **In NetWare® Administrator, select the Dial Access System object.**
2. **Select Object > Details > Remote Connections.**
3. **Select Limit Connections, specify the number of concurrent dial-in restrictions, then click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting the Current Connection Interval

To set the current connection interval, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Remote Connection Restrictions.**
3. **Enter a value (in days) and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting the Interim Accounting Timeout Interval

To set the interim accounting timeout interval, complete the following steps:

1. **In NetWare® Administrator, select the Dial Access System object.**
2. **Select Object > Details > Remote Connection Restrictions.**
3. **Enter a value (in minutes) and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting the Maximum Records in the Remote Connection History

To add concurrent login restrictions, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Remote Connection Restrictions.**
3. **Enter a value and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Specifying Per-User Login Restrictions

You can accept the default number of concurrent dial-in connections that the RADIUS server will allow for each User object (as specified for a given Dial Access System object), or you can override the default value for a given User object to either specify a different number of concurrent dial-in connections or allow unlimited dial-in connections.

For a given User object, the following types of information are tracked automatically:

- Active connections
- Login connection history

Setting User Remote Connections Restrictions

To add remote connections restrictions, complete the following steps:

1. **In NetWare Administrator, select the User object.**
2. **Select Object > Details > Remote Connections.**
3. **Specify the login restrictions and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Planning Token Authentication

To configure tokens for a particular vendor, you must perform a series of procedures. Use the following list to ensure you perform all the required procedures:

- ☐ Create an Authentication Container object.

You must create at least one Authentication Container object for each vendor you support.

- ☐ Initialize the tokens.

You must initialize or program each token with the profile parameters.

The initialization information must also be stored in NDS™ in an Authentication Device object. There are three methods to initialize tokens, create an Authentication object, and store the data in NDS:

- Import factory initialization data (device images) on preinitialized tokens from a disk into NDS.
- Locally initialize the token by selecting the parameters in NetWare® Administrator and downloading the data to the token using special initialization hardware.
- Manually initialize the token by selecting the parameters in NetWare Administrator and manually keying in the initialization codes from the keypad.

- ☐ Assign the tokens.

You can assign tokens to users from the Authentication Device object page or from the User object page.

- ☐ Configure token authentication in the Dial Access System object.

You must configure the Dial Access System object policy to allow token authentication as a method.

- ☐ Grant rights to access token objects.

You must grant the appropriate rights to the Dial Access System object to access the token objects.

Authentication Container Object

The Authentication Container object contains the Authentication Device objects (tokens or smart cards) from a single vendor and manages the common configuration tasks for these objects. All Authentication Device objects must be contained within an Authentication Container object. Therefore, you must create at least one Authentication Container object for each vendor you support. You may create multiple Authentication Container objects if you would like to store the Authentication Device objects from a vendor in more than one location in NDS. This object consists of the following pages:

- **Identification**—Identifies the name of the Authentication Container object and the type of tokens (from what vendor) that are contained in the object.
- **Import Device Images**—Lets you to import the device images containing the initialization information of a series of factory-preinitialized tokens. For each device image you import, a device object in NDS is automatically created.
- **Manual Initialization**—Lets you to initialize a token by generating and displaying the necessary initialization codes for you to enter manually into the token keypad. When you manually initialize a token, if the device object does not already exist in NDS, one is automatically created.
- **Local Initialization**—Lets you to initialize a token which you have placed in the token initializer hardware attached locally to your administration workstation. When you locally initialize a token, if the device object does not already exist in NDS, one is automatically created.
- **Token Assignment**—Lets you to assign devices to users. You can use this page to assign a single token to a user, or quickly assign a series of serialized tokens to a series of users.

Authentication Device Object

The Authentication Device object contains information about a single token or other device. When you import or initialize a token, an Authentication Device object is created. This object contains the following pages:

- **Identification**—Identifies the token name, assigned user, type, and status.

- **Assignment**—Lets you assign the token to a user and enable or disable the token.
- **Synchronize**—Lets you synchronize the token. You have the option of synchronizing the token manually or automatically the next time the token is used. For manual synchronization, you must specify the event, clock value, or both.
- **Password Tests**—Lets you test the token to verify that it can correctly generate a password. You can test both the synchronous and asynchronous methods of password generation.

Protecting Device Data in NDS

The authentication device data stored in NDS is critical to system security. This data should be carefully protected and access to it should be restricted to authentication servers and administrators who require access.

Sensitive information stored on authentication device objects is encrypted automatically; however, additional measures should be taken to protect this data. We recommend the following:

- Create a partition at the authentication device container
- Restrict replication of authentication device partitions to a few servers that are well controlled
- Ensure that backup copies of authentication device objects are protected
- Create access controls to allow administrators and Dial Access System objects to read and write these objects
- Block inherited rights and ensure access control lists (ACLs) are only for objects that should have access

Managing Token Authentication

Novell® BorderManager™ Authentication Services enables you to use NDS™ as the database to manage token authentication. Using the NetWare® Administrator utility on the administration workstation, you can perform the following management tasks:

- “Creating an Authentication Container Object” on page 18
- “Creating an Authentication Device Object” on page 19
- “Importing a Token” on page 19
- “Manually Initializing a Token” on page 19
- “Locally Initializing a Token” on page 20
- “Assigning a Single Token” on page 20
- “Assigning a Series of Tokens” on page 21
- “Synchronizing a Token” on page 21
- “Unlocking a Token” on page 21
- “Testing Passwords” on page 22

Creating an Authentication Container Object

To create an authentication container, complete the following steps:

1. **In NetWare Administrator, select Object > Create > Authentication Container.**
2. **Specify the name of the authentication container and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Creating an Authentication Device Object

To create an authentication device object, complete the following steps:

1. **In NetWare Administrator, select Object > Create > Authentication Device.**
2. **Specify the name of the authentication device and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Importing a Token

To import a token, complete the following steps:

1. **In NetWare Administrator, select the authentication container object.**
2. **Select Object > Details > Import Device Images and browse to the file that contains the token device image to import.**
3. **Click Import Images > Create Objects Now > OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Manually Initializing a Token

To manually initialize a token, complete the following steps:

1. **In NetWare Administrator, select the authentication container object.**
2. **Select Object > Details > Manual Initialization and specify the following information:**
 - Profile
 - Language
 - Token serial number
 - Token initial PIN

3. Click Initialize Device > Create Object Now.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Locally Initializing a Token

To locally initialize a token, complete the following steps:

- 1. In NetWare Administrator, select the authentication container object.**
- 2. Select Object > Details > Local Initialization and specify the following information:**
 - Profile
 - Language
 - Token type
 - Serial port
 - Welcome message
 - Token initial PIN
- 3. Click Initialize Device > Create Object Now.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Assigning a Single Token

To assign a single token, complete the following steps:

- 1. In NetWare Administrator, select the authentication device object.**
- 2. Select Object > Details > Assignment and browse to the User object to assign the token.**
- 3. Click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Assigning a Series of Tokens

To assign a series of tokens, complete the following steps:

1. **In NetWare Administrator, select the authentication container object.**
2. **Select Object > Details > Token Assignment and specify the following information for each token:**
 - Token serial number
 - User name
3. **Click Assign Now.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Synchronizing a Token

To synchronize a token, complete the following steps:

1. **In NetWare Administrator, select the authentication device object.**
2. **Select Object > Details > Synchronization and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Unlocking a Token

To unlock a token, complete the following steps:

1. **In NetWare Administrator, select the authentication device object.**
2. **Select Object > Details > Unlock Code.**

3. **Enter the challenge code displayed by the token and click Unlock Now.**
4. **Enter the response code into the token.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Testing Passwords

To test an asynchronous password, complete the following steps:

1. **In NetWare Administrator, select the authentication device object.**
2. **Select Object > Details > Password Tests > Asynchronous > Test Now and enter your PIN.**
3. **Enter the challenge code into the token.**
4. **Enter the password and click OK.**

To test a synchronous password, complete the following steps:

1. **In NetWare Administrator, select the authentication device object.**
2. **Select Object > Details > Password Tests > Synchronous > Test Now and enter your PIN.**
3. **Enter the password and click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Planning Authentication Policies

All users accessing services through Novell® BorderManager™ must be authenticated. All authentication, regardless of which BorderManager service is being accessed, is processed by a special module, the Authentication Device Manager (ADM), that authenticates users for the following services:

- Virtual Private Networks (VPN)

- Proxy Services
- SOCKS
- Dial-In Authentication Services

The authentication policies enforced by the ADM are defined and stored in an NDS™ object called the Authentication Policy object (APO). The APO contains authentication rules that define the relationships among the services, users, and authentication methods so that the ADM can determine and enforce the appropriate authentication requirements.

Authentication Device Manager

All BorderManager servers must load the ADM. On each BorderManager server object, an attribute specifies the Authentication Policy object that contains the authentication rules to be enforced on that server. If ADM is loaded and no Authentication Policy object is specified, then the ADM loads but does not process authentication requests. Therefore, until a Authentication Policy is set, access to BorderManager from any service is not available.

Important You must set up a generic authentication policy to allow all users to access network services through each of the various BorderManager services. See *Novell BorderManager Enterprise Edition 3.5 Installation and Setup* for more information.

When a particular service needs to authenticate a user, that service calls the ADM and passes the necessary information about itself (such as its service ID) and the user, container, or group object (the distinguished name and credentials) for the ADM to process the request. The ADM uses this information to determine the applicable authentication rule from the rule set stored in the Authentication Policy object, and then enforces that rule set.

Authentication Policy Object

Authentication rules or policies are defined and stored in NDS in the Authentication Policy object. This allows you to define policies that can be used locally (on a single server), or globally (across multiple servers and services throughout the NDS tree).

Note You will usually need only one Authentication Policy object for each NDS replica.

The Authentication Policy object is administered through NetWare® Administrator. This object enables you to set up authentication rules that allow you to manage authentication for the following BorderManager service types:

- VPN
- Proxy Services
- SOCKS
- Dial-In Authentication Services
- All services (includes VPN, proxy services, SOCKS, and dial-in authentication services)

To define a rule for a service type, you must select the service type from NetWare Administrator. The VPN, Proxy Services, and SOCKS service types are predefined. The Authentication Services service type is represented by an NDS Dial Access System (DAS) object. To define a rule for Authentication Services, you must select the distinguished name of the DAS object associated with the service.

Supported Authentication Methods

BorderManager supports a variety of authentication methods. The exact methods supported depend on the service type. The following table lists the authentication methods supported for each service type.

Table 1-1

Authentication Methods Supported

Service Type	Authentication Methods Supported
Proxy Services	Any user-assigned device
	NDS passwords
	Token-based authentication methods
SOCKS	Any user-assigned device
	NDS passwords
	Token-based authentication methods
VPN	Any user-assigned device
	NDS passwords (mandatory)
	Token-based authentication methods
	NOTE: When token-based authentication is selected, the VPN client will be required to supply both a token password and an NDS password
Authentication Services	Any user-assigned device
	NDS passwords
	Token-based authentication methods
	Dial access passwords (PAP)
	Dial access passwords (CHAP)

Authentication Rules

Authentication rules define the authentication method required for a specific user, container, or group object to access a particular BorderManager service. When a user requests access, the applicable rule will be enforced. You can define a single authentication rule for all BorderManager services, or different authentication rules for the different BorderManager service types. If you define multiple authentication rules, the rules are applied in the order in which they appear in the list. Once a rule has been matched, no other rules are evaluated. To change the priority of a rule, simply change its position in the list.

You can also define the level of enforcement for a rule. The following enforcement levels are defined:

- **Mandatory**—The user must authenticate using this method.
- **Required if assigned**—The user is required to authenticate using this method if one is assigned for them.
- **Optional**—The user may authenticate using this method.

The following table illustrates some possible authentication rules.

Table 1-2
Authentication Rule Examples

Service	Users	Authentication Method	Enforcement
<VPN>	.hr.acme	<NDS password>	Mandatory
		.token.acme	Mandatory
<Proxy>	.sales.acme	.token.acme	Required if assigned
		<NDS password>	Mandatory
<SOCKS>	<Any>	.token.acme	Required if assigned
.das.acme	<Any>	.token.acme	Required if assigned
		<NDS password>	Mandatory
<Any>	<Any>	<NDS password>	Mandatory

Setting Up Authentication Policies

To set an authentication policy for Novell® BorderManager™ Authentication Services, complete the following tasks:

- “Creating an Authentication Policy Object” on page 27
- “Defining the Server to Host the Authentication Policy Object” on page 27

- “Configuring Authentication Policy Rules” on page 27

Creating an Authentication Policy Object

To create an Authentication Policy object, complete the following steps:

1. **In NetWare® Administrator, select the Organization or Organizational Unit object where you want to place the Authentication Policy object.**
2. **Select Create from the Object menu.**
3. **Select Authentication Policy and click OK.**
4. **Enter the name of the Authentication Policy object and click OK.**

Defining the Server to Host the Authentication Policy Object

To define the servers using the Authentication Policy object, complete the following steps:

1. **In NetWare Administrator, select the Authentication Policy object and right-click Details.**
2. **Select Hosts > Add.**
3. **Browse to select the server object that will host the Authentication Policy object and click OK.**

Configuring Authentication Policy Rules

To configure authentication policy rules, complete the following steps:

1. **In NetWare Administrator, select the Authentication Policy object and right-click Details.**
2. **Select Rules > Add.**
3. **Select a predefined Service Type, or browse to select the distinguished name of a Service object.**

4. **Click Users, add the User objects or Group objects that will use the policy, then click OK.**
5. **Click Methods > Add.**
6. **Select the Authentication Method Type.**
7. **(Optional) If you selected the Distinguished Name authentication method, browse and select the authentication method container.**
8. **Select the appropriate Method Enforcement.**
9. **Check Decrement Grace Logins if desired, and click OK.**
10. **Use the Up and Down arrows to specify the priority that the methods will be used (first to last).**

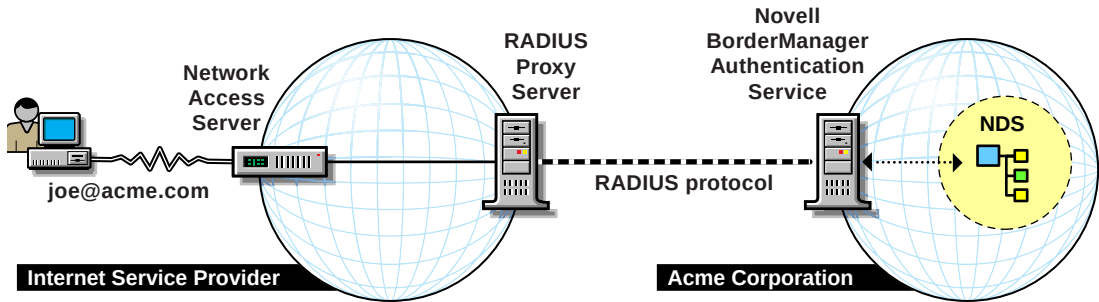
Planning RADIUS Proxy Services

You can use RADIUS proxy to outsource the management of dial-in hardware to an Internet Service Provider (ISP) while you manage the users in your NDS™ tree. This benefit provides you with the flexibility to manage dial-in users without the investment in dial-in hardware or the burden of managing the hardware.

Using RADIUS proxy, a remote user (such as jane@acme.com) dials in to an ISP network. The user's access request (user ID and password) is forwarded to a RADIUS proxy server on the ISP network. The ISP RADIUS proxy server forwards the access request to your company's RADIUS server (such as acme.com). The RADIUS server then checks the information in the access request and either accepts or rejects the request. If the RADIUS server accepts the request, it returns configuration information specifying the type of connection service (such as PPP or Telnet) to deliver to the user.

This concept is shown in Figure 1-1.

Figure 1-1
RADIUS Proxy



The RADIUS server provided with Novell® BorderManager™ Authentication Services can act as both a conventional RADIUS server and a RADIUS proxy server at the same time. To set up a RADIUS proxy, you must add a domain to the Dial Access System object's domain list. The domain name you assign is the target domain the user must use to be directed to that proxy for authentication. The RADIUS server supports usernames specified as either an NDS distinguished name or a common name. For access requests that have a username without a domain, you can configure search domains that can be checked to determine if valid authentication information is available. The search domains consist of configured domains that do not authenticate by NDS context. Domains are defined as one of the following types:

- **NDS Context—Any BorderManager Authentication Services server**

This domain type configures an authentication domain for the Dial Access System object that will look up users by NDS context. The authentication request can be processed by any BorderManager Authentication Services server in the NDS tree. For this domain type, you specify the NDS context and define whether to look for the user in that context and any context under it, or look for the user only in the specified context. If the user is not found, you can set the option to look up the user in any defined search domains.
- **NDS Context—Specific BorderManager Authentication Services server**

This domain type also configures an authentication domain for the Dial Access System object that will look up users by NDS context. However, this domain type will forward the authentication request to a specific BorderManager Authentication Services server in the NDS tree where the user belongs to reduce network latency. For this domain type, you specify the NDS context and define whether to look for the user in that

context and any context under it, or look for the user only in the specified context. The search domain option is not available. To define the target server, specify the IP address, port, and RADIUS secret of the server. To define how accounting packets are handled, specify whether to log accounting locally on the server or forward accounting packets to an accounting server on a remote domain.

- Generic proxy server

This domain type configures a simple domain proxy. Authentication requests will be forwarded to the designated RADIUS server. If the server expects to see only the common username, set the option to remove the target domain name the user logged in with. To target the server, specify the IP address, port, and RADIUS secret for the server. To define how accounting packets are handled, specify whether to log accounting locally on the server or forward accounting packets to an accounting server on a remote domain.

- Search Domain Server

This domain type configures a search domain. Search domains are searched when a user logs in with a common username (no target), or when a user with a target domain is not found in a specified NDS context and usage of a search domain is allowed for that domain. If the server expects to see only the common username, set the option to remove the target domain name the user logged in with. To target the server, specify the IP address, port, and RADIUS secret for the server. To define how accounting packets are handled, specify whether to log accounting locally on the server or forward accounting packets to an accounting server on a remote domain.

- External Authentication Service Object

This domain type configures a domain that targets an external authentication server (such as a Security Dynamics ACE/Server). If the server expects to see only the common username, set the option to remove the target domain name the user logged in with. To target the server, specify the IP address, port, and RADIUS secret for the server. You can create External Identity objects for third-party tokens administered by an External Authentication Service object and assign NDS users to an External Identity object.

Refer to the NetWare® Administrator online help for information about specific configuration procedures.

This section contains the following tasks:

- “Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS Context to Any RADIUS Server” on page 31
- “Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS Context to a Specific RADIUS Server” on page 32
- “Setting Up a RADIUS Authentication Proxy as an ISP to Forward Requests to a Corporate RADIUS Server” on page 32
- “Setting Up a RADIUS Authentication Proxy to Forward Requests to a Third-Party Authentication Server Supporting Token Authentication” on page 33
- “Setting Up a RADIUS Authentication Proxy to Forward Requests to Third-Party Authentication Server Supporting Token Authentication with Token Serial Numbers as Usernames” on page 34
- “Setting Up a RADIUS Authentication Proxy to Authenticate Usernames to a Search Domain” on page 34

Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS Context to Any RADIUS Server

A user logs in as jane@acme.com. You want this user to authenticate using the local NDS tree and search for the user from the [Root] context of the NDS tree and any context below [Root]. You don't care which RADIUS server handles the authentication. If the user cannot be authenticated in the NDS tree, you want the server to send the authentication request to all the search domains for the Dial Access System object. Configure the Dial Access System object as follows:

Domain Name: acme.com

Domain Type: NDS Context—Any BMAS Server

NDS Context Name: [Root]

Look for user in any lookup context under this context: checked

Use search domains if user not found: checked

Refer to the NetWare Administrator online help for information about specific configuration procedures.

Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS Context to a Specific RADIUS Server

A user logs in as jane@sales.acme.com. You want this user to authenticate using the local NDS tree, but you want to search for the user only in the sales.acme context. You also want a specific RADIUS server that is within the same partition of the NDS tree as the sales context to handle the authentication to reduce network latency for the login. The IP address for the RADIUS server is 1.2.3.4 and the secret is 12345678998765432100. You need the accounting to be logged locally on the RADIUS server. Configure the Dial Access System object as follows:

Domain Name: sales.acme.com

Domain Type: NDS Context—Specific BMAS Server

NDS Context Name: sales.acme

Look for user in this context only: checked

Primary Address: 1.2.3.4 Port: 1645

Secret: 12345678998765432100

Log at proxy server: checked

Refer to the NetWare Administrator online help for information about specific configuration procedures.

Setting Up a RADIUS Authentication Proxy as an ISP to Forward Requests to a Corporate RADIUS Server

You manage an ISP. Acme Corporation user joe dials in with the username joe@acme.com, and you need to forward the authentication request to the corporation's RADIUS server at IP address 1.2.3.4, port 1645, with a RADIUS secret of 12345678998765432100. You also need to forward accounting to the Acme corporation RADIUS accounting server at IP address 1.2.4.5, port 1646, with a RADIUS secret of 98765432112345678900 and a retry limit of 24 hours. Configure the Dial Access System object as follows:

Domain Name: acme.com

Domain Type: Generic Proxy

Primary Address: 1.2.4.5 Port: 1645

Secret: 12345678998765432100

Forward to domain: checked

Use alternate addresses/secret: checked

Primary Address: 1.2.4.5 Port: 1646

Secret: 98765432112345678900

Refer to the NetWare Administrator online help for information about specific configuration procedures.

Setting Up a RADIUS Authentication Proxy to Forward Requests to a Third-Party Authentication Server Supporting Token Authentication

Your corporation has a Security Dynamics ACE/Server external server that supports token authentication. Your sales force uses this token implementation extensively and you need to preserve your investment in this hardware. You want to use the token authentication capabilities of this server, but would like to manage the users in NDS with BorderManager Authentication Services. Salesperson Olivia Olsen logs in as Olivia.Sales.Acme. You want to remove the domain name on this login and create a domain, ace, to forward the request to the external authentication server at IP address 1.2.3.4, port 1645, with a RADIUS secret of 09876543211234567890. To implement this example, you must create an External Authentication Service object and an External Identity object.

Configure the External Authentication Service object as follows:

Domain Name: ace

Domain Type: External Authentication Server

Remove domain name: checked

Primary Address: 1.2.3.4

Port: 1645

Secret: 09876543211234567890

Accounting Log at proxy server: checked

Assign the User object to the External Identity Object as follows:

Login Name: Olivia.Sales.Acme

Given Name: Olivia

Last Name: Olsen

Refer to the NetWare Administrator online help for information about specific configuration procedures.

Setting Up a RADIUS Authentication Proxy to Forward Requests to Third-Party Authentication Server Supporting Token Authentication with Token Serial Numbers as Usernames

Your implementation is exactly the same as in the previous configuration; however, you want to eliminate the need to manage user accounts on the token server. Instead of using usernames on your external authentication server, you have assigned the serial number of the token as the login name. The serial number and login name for the token used by salesperson Olivia Olsen is 12345. You still want Olivia to log in as Olivia.Sales.Acme. However, you want NDS to substitute 12345 as Olivia's other name. To implement this configuration, you must configure the User object Olivia as follows:

Login Name: Olivia.Sales.Acme

Given Name: Olivia

Last Name: Olsen

Other name: 12345@ace

Configure the External Authentication Service object as follows:

Domain Name: ace

Primary Address: 1.2.3.4

Port: 1645

Secret: 09876543211234567890

Refer to the NetWare Administrator online help for information about specific configuration procedures.

Setting Up a RADIUS Authentication Proxy to Authenticate Usernames to a Search Domain

Acme Corporation has a legacy RADIUS server. You want to migrate your remote access to BorderManager Authentication Services; however, you want to do it gradually, moving one department a month from the legacy system to BorderManager. You want your users to authenticate to the BorderManager RADIUS server and you want this server to search the legacy RADIUS server if the user does not exist in NDS.

To allow users to authenticate, you can set up a search domain on the BorderManager Authentication Services RADIUS server. The legacy RADIUS server, RAD1, is at IP address 1.2.3.4, port 1645, with a secret of

09876543211234567890. You also want accounting to be logged at the legacy proxy server. Configure the Dial Access System object on the BorderManager Authentication Services RADIUS server as follows:

Domain Name: RAD1
Domain Type: Search Domain Server
Primary Address: 1.2.3.4
Port: 1645
Secret: 09876543211234567890
Accounting Log at proxy server: checked

Refer to the NetWare Administrator online help for information about specific configuration procedures.

Managing RADIUS Proxy Services

Using the NetWare® Administrator utility on the administration workstation, you can perform the following management tasks for RADIUS proxy services:

- “Adding an NDS Context Domain Processed by Any RADIUS Server” on page 36
- “Adding an NDS Context Domain Processed by a Specific RADIUS Server” on page 36
- “Adding a Generic Proxy Server Domain” on page 37
- “Adding a Search Domain Server Domain” on page 37
- “Adding a RADIUS Accounting Proxy Domain” on page 38
- “Adding an External Authentication Service Object” on page 38
- “Adding an External Identity Object” on page 39
- “Modifying a Domain” on page 39
- “Deleting a Domain” on page 39

Adding an NDS Context Domain Processed by Any RADIUS Server

To add an NDS™ context domain to be processed by any RADIUS server, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Add and enter the name of the authentication domain.**
3. **Select Domain Type > Any BMAS Server and browse to the name of the NDS context to search.**
4. **Click OK twice.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding an NDS Context Domain Processed by a Specific RADIUS Server

To add an NDS context domain to be processed by a specific RADIUS server, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Add and enter the name of the authentication domain.**
3. **Select Domain Type > Specific BMAS Server and browse to the name of the NDS context to search.**
4. **Specify the IP address and TCP port number of the specific RADIUS server.**
5. **Enter and re-enter the RADIUS secret.**
6. **Click OK twice.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding a Generic Proxy Server Domain

To add a generic proxy server domain, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Add and enter the name of the authentication domain.**
3. **Select Domain Type > Generic Proxy Server.**
4. **Specify the IP address and TCP port number of the RADIUS server.**
5. **Enter and re-enter the RADIUS secret.**
6. **Click OK twice.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding a Search Domain Server Domain

To add a search domain server domain, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Add and enter the name of the authentication domain.**
3. **Select Domain Type > Search Domain Server.**
4. **Specify the IP address and TCP port number of the RADIUS server.**
5. **Enter and re-enter the RADIUS secret.**
6. **Click OK twice.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding a RADIUS Accounting Proxy Domain

To add a RADIUS accounting proxy domain, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Domains and specify the following information:**
 - Accounting > Forwarding
 - Retry Limit
3. **Click OK twice.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding an External Authentication Service Object

To add an External Authentication Service object, complete the following steps:

1. **In NetWare Administrator, select the NDS tree.**
2. **Select Create > External Authentication Service.**
3. **Enter the name of the External Authentication Service object.**
4. **Check Define Additional Properties to assign additional properties to the External Authentication Service object during creation.**
5. **Specify the IP address and TCP port number of the external RADIUS server.**
6. **Enter and re-enter the RADIUS secret.**
7. **Click OK twice.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding an External Identity Object

To add an External Identity object, complete the following steps:

1. **In NetWare Administrator, select the External Authentication Service object.**
2. **Select Create > External Identity.**
3. **Enter the name of the External Identity object.**
4. **Check Define Additional Properties to assign additional properties to the External Authentication Service object during creation.**
5. **Click OK twice.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Modifying a Domain

To modify a domain, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Domains and select the domain name to modify.**
3. **Click OK.**

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Deleting a Domain

To delete a domain, complete the following steps:

1. **In NetWare Administrator, select the Dial Access System object.**
2. **Select Object > Details > Domains and select the domain name to delete.**

3. Click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Displaying RADIUS Status Messages

The Novell® BorderManager™ Authentication Services status display provides status messages that are helpful in troubleshooting user access problems. You can view the status display in the following ways:

- From the NetWare® (version 4.11 or later) server console, enter the following commands to control the status display:

```
RADIUS display {on|off}  
RADIUS display {+|-} {failure|success}  
RADIUS SystemLog {on|off}  
RADIUS SystemLog file_location  
RADIUS SystemLogSize new_size  
RADIUS SystemLogPolicy [daily|weekly|days]  
RADIUS LogStatus
```

- When a BorderManager Authentication Services server is started, the status window displays only messages for authentication failures. Descriptions of failure messages are listed in the following categories:
 - Access Rejected Messages
 - Messages Dropped Messages
 - Other Messages

Each message is listed with the possible causes.

Access Rejected Messages

Device not enabled

The authentication device has not been enabled for use.

Device not present

The authentication device was not detected.

Exceeded concurrent login limit

The number of remote connections has exceeded the limit specified in the Dial Access System object or User object.

Invalid password

Possible causes:

- User entered the wrong password.
- Shared secret does not match between the network access server and the RADIUS server. The shared secret is case sensitive.
- Client workstation attempted to authenticate using the Challenge Handshake Authentication Protocol (CHAP), but the password policy was set to use an NDS™ password. (CHAP authentication requires a separate dial access password.)

Login disabled

The user NDS account has been disabled on the login restriction page.

Method not allowed

The specified authentication method is not permitted by the Authentication Device Manager.

Method not supported

The Authentication Device Manager does not support the authentication method.

No authentication policy configured

No authentication policy has been configured for the Dial Access System object.

No devices assigned

No authentication device has been assigned to the User object.

No more search domains

All search domains defined for a Dial Access System object have been searched without success.

No service data

No service data is available for the authentication device.

No such context

The specified NDS context does not exist.

No such domain

The domain name is not defined on the Dial Access System object.

No such profile

The Dial Access System object does not have Browse and Read rights to the Dial Access Profile object.

No such proxy target

No entry exists in the proxy target page for the domain that the user entered.

No such service tag

No service is defined for the User or container object that matches the service tag entered by the user.

No such user

Possible causes:

- User object does not exist.
- Lookup context does not exist.
- User entered the username incorrectly (distinguished name syntax error).

- Dial Access System does not have Browse and Read rights to the User object.

Password expired

The NDS password has expired.

Proxy rejected

The target RADIUS server rejected the authentication request. Consult the output of the final RADIUS server in the proxy chain to determine the problem.

Unknown method tag

The authentication method tag is not defined for the Dial Access System object.

User not a member of dial access system

Possible causes:

- Dial Access System object does not have Browse and Read rights to the User object or container object.
- Dial Access System object has not been specified for the User or container object.
- User or container object has been configured to use a different Dial Access System object.

User not enabled for RADIUS login

Possible causes:

- Dial access is disabled on the User object.
- Dial access is disabled on the container object for a User object using the container setting.
- Dial Access System object does not have Browse and Read rights to the User object or container object.

Message Dropped Messages

Proxy loop detected

The chain of proxy RADIUS servers has been configured in a loop. A loop is an invalid configuration. Check your proxy target configuration to ensure that no loops occur.

Unknown RADIUS client

No entry exists in the Dial Access System client table for the RADIUS client that issued the access request.

Other Messages

RADIUS Error -150

Insufficient Memory

A system error has occurred (sufficient memory was not available to satisfy the current memory allocation request).

RADIUS Error -307

Missing NDS Replica

The NDS replica that the RADIUS server is using failed.

RADIUS Error -601

The Dial Access System object is not valid.

RADIUS Error -672

The user does not have sufficient rights to perform this operation.

RADIUS Error -801

Insufficient Buffer

An internal failure occurred (the system allocated a buffer of insufficient size).

RADIUS Error -802

Invalid Request

An invalid request was received.

RADIUS Error -803

No Such Attribute

Possible causes:

- A requested RADIUS attribute was not found.
- An invalid attribute was detected in an incoming RADIUS message.

RADIUS Error -804

Invalid Data

Malformed data was detected in the NDS directory.

RADIUS Error -805

Invalid Transport

The host system is not configured properly for TCP/IP.

RADIUS Error -806

Invalid Signature

The signature on a proxy reply message is invalid.

RADIUS Error -807

Invalid Data Version

Unknown data was found in the NDS directory.

RADIUS Error -808

Proxy Loop Detected

The chain of proxy RADIUS servers has been configured in a loop. A loop is an invalid configuration. Check your proxy target configuration to ensure that no loops occur.

RADIUS Error -809

Invalid Parameter

An invalid parameter value was specified.

ADM Error 900

Device Already Supported

The authentication device is already defined.

ADM Error 901

Invalid Structure Version

An invalid version was specified.

ADM Error 902

Invalid Request Entry Point

An invalid request was specified.

ADM Error 903

Device Not Present

The authentication device is not present.

ADM Error 904

Method Tag Already Supported

The authentication method tag has already been defined.

ADM Error 905

Invalid Snap-In Handle

The snap-in handle is not supported.

ADM Error 906

Invalid Subject

The subject is not supported.

ADM Error 907

Unknown Method Tag

The authentication method is not supported.

ADM Error 908

Method Not Allowed

This authentication method is not permitted.

ADM Error 909

Invalid Policy Count

An invalid policy count was specified.

ADM Error 910

Invalid Service Count

An invalid service count was specified.

ADM Error 911

Invalid Policy Type

This authentication policy is not supported.

ADM Error 912

Method Not Supported

This authentication method is not supported.

ADM Error 913

No Devices Assigned

No authentication devices have been assigned to a User object.

ADM Error 914

No Default Device

No default authentication device has been specified.

ADM Error 915

No Service Data

No service data is available.

ADM Error 916

Invalid State

The authentication device is in an invalid state.

ADM Error 917

Snap-In Registration Table Empty

An error occurred to the snap-in registration table.

ADM Error 918

Memory Allocation

A memory allocation error has occurred.

ADM Error 919

Unable to Locate Snap-in

The snap-in module cannot be found.

ADM Error 920

Invalid NDS Response

An invalid NDS response was received.

ADM Error 921

Unsupported Version

An unsupported version is being used.

ADM Error 922

No Such Attribute

This attribute is not supported.

ADM Error 923

Invalid Encryption Type

This encryption type is not supported.

ADM Error 924

Invalid Service Tag

This service tag is not supported.

ADM Error 925

Invalid Object DN

The distinguished name for the object is not valid.

ADM Error 926

Unable to Locate Pending Request

A pending authentication request cannot be located.

ADM Error 927

Unable to Load Snap-In

The snap-in module cannot be loaded.

ADM Error 928

Unable to Retrieve Required Data

The required data cannot be retrieved.

ADM Error 929

Shutdown in Progress

The program is being shut down.

ADM Error 930

Device Not Enabled

The authentication device is not enabled.

ADM Error 931

Invalid Buffer Size

An invalid buffer size was specified.

ADM Error 932

Invalid Authentication Materials

An invalid configuration was supplied.

ADM Error 933

Unsupported Cryptography Algorithm

This cryptography algorithm is not supported.

ADM Error 934

Invalid Password

An invalid password was specified.

ADM Error 935

Login Disabled

Login for the user is disabled.

ADM Error 936

Account Expired

The user account has expired.

ADM Error 937

Password Expired

The supplied password has expired.

ADM Error 938

Intruder Detection

An intruder has been detected.

